Communications Security Establishment Commissioner

Canada

Office of the Communications Security Establishment Commissioner
P.O. Box 1984
Station 'B'
Ottawa, Ontario
K1P 5R5

Tel: (613) 992-3044
Fax: (613) 992-4096

© Minister of Public Works and Government Services Canada 2000
ISSN 1206-7490
Cat. No. D95-2000

100-05508/

Communications Security Establishment Commissioner

The Honourable Claude Bisson, O.C.

CANADA

Commissaire du Centre de la sécurité des télécommunications

L'honorable Claude Bisson, O.C.

May 2000

The Honourable Arthur C. Eggleton, P.C.
Minister of National Defence
MGen G.R. Pearkes Building, 13th Floor
101 Colonel By Drive, North Tower
Ottawa, Ontario
K1A 0K2

Dear Mr. Eggleton:

Pursuant to paragraph (g) of Order in Council P.C. 1999-1048 re-appointing me Communications Security Establishment Commissioner, I am pleased to submit to you my 1999-2000 annual report on my activities and findings, for your submission to Parliament.

Yours sincerely,

Claude Bisson

P.O. Box/C.P. 1984, Station "B"/Succursale -B-
Ottawa, Canada
K1P 5R5
(613) 992-3044 Fax: *(613)* 992-4096

TABLE OF CONTENTS

A New Mandate 1

1999-2000 Review Undertakings 2

- Internal Investigations and Complaints 2
- Foreign Signals Intelligence 2

  The Intelligence Cycle 3

  'Second Party' Collection 5
- Information Technology Security 6

Budget and Staff 7

1999-2000 Findings 8

The Complaints Function 9

- Anonymous Allegations 9

Building Relationships 10

- DND Ombudsman 10
- International Conference 11

The Future of Review for CSE 12

My New Website 13

People and Places 13

Annex: Order in Council P.C. 1999-1048 15

A New Mandate

For the past four years I have had the responsibility of reviewing the activities of the Communications Security Establishment (CSE) and reporting to the Minister of National Defence on the lawfulness of those activities.

My initial three-year mandate was set out in a 1996 Order in Council of the Government of Canada under the *Inquiries Act*. On June 15, 1999, the Minister of National Defence announced that the government had renewed my appointment for another three years and enhanced my mandate by increasing my authority to respond to complaints about CSE. A copy of the new Order in Council appears as Annex A of this report.

This Annual Report – my fourth – covers the first year of my second mandate, up to the government's fiscal year end of March 31, 2000.

The task of reviewing CSE is an important and necessary one in a democratic society. An agency of Canada's Department of National Defence, CSE provides the Government of Canada with foreign signals intelligence (SIGINT), which it obtains by gathering and analyzing foreign radio, radar and other electronic emissions. Through its Information Technology Security program, CSE also provides advice on the security of the government's information technology.

To fulfil its mandate, CSE has, over the more than five decades of its existence, developed highly sophisticated technological capabilities. One of my functions is to review CSE's activities to ensure that the organization does not use its capabilities in ways that contravene the laws of Canada.

1999-2000 Review Undertakings

During this past year, I submitted four classified reports to the Minister of National Defence. One of these reports revisited the subject of internal investigations and complaints. The remaining reports presented the results of reviews of CSE activities related to its foreign signals intelligence and information technology security mandates. All studies included an examination of the legal parameters within which CSE operates, related policies and practices, and the accountability systems and procedures in place at CSE. None revealed issues of unlawful activity.

Internal Investigations and Complaints

When I first reviewed CSE's internal investigations and complaints in 1997-98, I observed that most dealt with such issues as security infractions, and none involved unlawful activity in the delivery of CSE's mandate. This was again the case this past year. In the interim, CSE implemented many new internal security policies and initiatives to heighten security awareness. These appear to have proven effective, in that there were far fewer incidents leading to internal investigations this past year than in 1997-98.

Foreign Signals Intelligence

In reviewing CSE's signals intelligence activities this past year, I noted a continuing enhancement and updating of SIGINT policies and directives in response to the evolving communications environment. I also observed new initiatives introduced by CSE to enhance its ability to manage and account for its SIGINT-related activities.

I paid particular attention this year to examining not only *what* CSE collects and retains, but *how* CSE's intelligence holdings are generated. As a result, I was able to further my knowledge and understanding of some of the highly specialized and technical means used to minimize the likelihood that private Canadian communications would make their way into CSE's

holdings. I am able to state that, as of this date, I am satisfied that, within the current technical environment, CSE is employing appropriate measures to safeguard the privacy of Canadians.

The Intelligence Cycle

In last year's report, I observed that CSE's activities are driven by its mandate to fulfil the foreign intelligence requirements established by the Government of Canada, not by the capabilities of the technology at hand.

Those requirements, in the form of foreign intelligence priorities for Canada's intelligence community, are set annually by a group of Cabinet ministers whose responsibilities touch on the country's security within Canada and abroad. The establishment of the Government of Canada's intelligence priorities is the first step in what the intelligence community calls the "intelligence cycle." It is worth examining that cycle briefly and looking at CSE's role in it.

The Government of Canada's foreign intelligence priorities form the basis of CSE's yearly SIGINT program. That is to say, these priorities are conveyed formally to CSE by the Deputy Secretary to the Cabinet, Security and Intelligence, Privy Council Office. CSE then uses these priorities to determine what information it seeks to obtain, either from its own activities or from the activities of its partner agencies in the United States, the United Kingdom, Australia, and New Zealand.

Concurrent with this, CSE must ensure that the appropriate steps are always taken to minimize the likelihood of intercepting the private communications of Canadians.

Next, CSE receives the inflow of intelligence traffic from multiple sources – its own and those of its partners. This traffic is then processed, analyzed

and assessed against the government's intelligence priorities. The resulting intelligence product is disseminated to the government departments responsible for protecting Canada's security, intelligence, economic and defence interests.

Intelligence dissemination is facilitated by knowledgeable CSE staff who provide a tailored and timely intelligence delivery service to some 800 senior decision makers in government on ongoing and emerging issues. This regular contact with the users of CSE's intelligence product ensures that requirements are updated and feedback is incorporated in the production process.

The intelligence cycle provides me with one framework for reviewing CSE's activities. I can examine the lawfulness of CSE's activities at each stage of the cycle. Through this work, I keep abreast of foreign intelligence collection capabilities and practices, signals processing, signals and intelligence analysis, and the dissemination of intelligence product to CSE's clients in government.

I believe the exploding yield of information carried by global communications networks increases the need to ensure that the privacy of Canadians is protected. I continue working to identify and understand the numerous technological initiatives that support intelligence gathering. I am also increasing my understanding of *how* some of these initiatives are applied. Within this intelligence cycle, however, my interest remains the identification and examination of any technical applications and initiatives CSE uses to *avoid*, or at least minimize, the likelihood of private Canadian communications making their way into CSE's holdings.

I am able to report that CSE has undertaken initiatives to advance its technological capability to ensure the protection of private Canadian communications. CSE is aware of both my interest in this area and the importance I attach to assessing compliance. I encourage CSE's research and development initiatives in this fast-paced technological environment.

'Second Party' Collection

As noted earlier, CSE receives signals intelligence gathered by other governments. CSE also contributes intelligence it collects to other governments. These partnership arrangements – with the United States, the United Kingdom, Australia, and New Zealand – were developed during the Second World War and maintained throughout the Cold War. Signals that are provided by one country to another are described as 'second party' collection.

The governments of the countries involved in this exchange of intelligence have policies to ensure the privacy of their citizens. In particular, each government has agreed not to undertake collection on behalf of a second party that would be illegal in the second party country. In other words, they do not do indirectly what they cannot do directly.

I have made a point of developing an understanding of these collaborative relationships, focusing not only on shared policies but also on actual practices. I have sampled the documentation and had access to some of the systems that support intelligence gathering and exchange. At this time I am satisfied that CSE is taking all reasonable steps to safeguard the privacy of Canadian communications.

Information Technology Security

Over the past four years, I have focused much of my effort on CSE's SIGINT activities. However, CSE has another important role in government – its Information Technology Security (ITS) mandate: CSE advises the government on how to maintain security in its use of information technology.

This year, my Office conducted an in-depth examination of the ITS program to determine whether its activities were lawful. The study involved, first, a review of CSE's ITS authorities and mandate as provided in direction given to the Chief, CSE. This was followed by an examination of the management control framework established to govern the conduct and performance of ITS activities. Step three was an analysis of the environmental factors and changing circumstances affecting the government's security requirements. Finally, strategies, plans, operations and projects were reviewed against the template established by the preceding steps to identify issues or activities for further exploration.

No evidence of unlawful activity was found. However, the study did reveal several pertinent facts:

- The trend in government and the private sector toward increased electronic business and service delivery is radically transforming the ITS program. Whereas previously the program's focus was the protection of classified information about a small number of government clients, now it is called upon increasingly to advise on protecting unclassified but sensitive information, including the electronic business transactions that underpin many government programs and operations.
- If Canadians are to have confidence in electronic commerce and the infrastructure that makes it possible, the government must have "made-in-Canada" solutions to security concerns. CSE is

well equipped to play a key role in this, but it must be given clear direction by government on this sensitive issue.

- For example, one effective means of confirming the security of information infrastructure is to attempt to penetrate the defences (e.g., to test so-called firewalls). This is called "ethical hacking." CSE does not conduct such penetrations of active systems because this could reveal personal data, with privacy implications. However, the result is that mission-critical information technology systems are not tested for the full range of threat scenarios facing those systems.

Henceforth, I will closely monitor ITS involvement in these activities to ensure they comply with prevailing constraints. I also would encourage the government to give CSE clear policy direction regarding the role it should play in ensuring the security of Canada's information infrastructure.

Budget and Staff

My annual budget allocation for the year 1999-2000 was augmented to $635,500 to provide for additional expenses, including counsel, in support of my expanded complaints function. I can report that actual expenses incurred were within budget.

In addition to two full-time staff, I have continued the practice established during my first mandate of hiring subject matter experts under contract. At present, I have six contractors performing specialized work under this arrangement, all of whom have been security cleared for the purpose of their work.

As I have indicated in the past, I believe I have adequate financial and personnel resources to carry out the mandate I have been given.

1999-2000 Findings

Based on the results of our review and analysis, I am of the opinion that CSE has acted lawfully in the performance of its mandated activities for the period under review. I am also satisfied that CSE has not targeted the communications of Canadian citizens or permanent residents of Canada.

These findings are consistent with those from previous years, since the creation of this Office. Through the process of study and review, I am advancing my knowledge and understanding of how CSE conducts its mandated activities. As my depth of knowledge increases, so does the certainty of my approach to assessing the lawfulness of these activities. Of particular importance to me is the increasing confidence with which I can state my findings.

By their very nature, foreign intelligence activities raise questions, and sometimes concerns, on the part of the private citizen. And I can attest to the technical, legal and ethical complexity of the intelligence cycle. I believe, therefore, that the existence of my Office since 1996 has been a necessary and appropriate addition to Canada's intelligence community. It has been my experience that, since 1996, CSE's policies, procedures and, most important, its practices have reflected the presence of my Office and my review parameters as established by the Government of Canada.

This combination of advancing capabilities on the part of my Office and improved policies and practices on the part of CSE augurs well for the future. Nevertheless, I intend to remain vigilant in reviewing the activities of CSE, and I will ensure that our increasing abilities are applied robustly as I fulfil the responsibilities of this Office.

The Complaints Function

This was the first year in which I had the authority to respond directly to individuals who raise complaints about CSE's activities. Previously, under my original mandate, I could receive such complaints but I was not able to report to the complainants about my findings. I was pleased when this limitation was removed when my mandate was renewed.

To help members of the public understand the role of my Office, and in particular the complaints function, we published a brochure, *Safeguarding the Privacy of Canadians*. The brochure notes that because complaints may contain sensitive information or may affect the privacy of Canadians, my Office will accept complaints only by mail, addressed to me. Copies of the brochure are available upon request.

My background and training in arbitration and mediation before I became Commissioner have made me a strong advocate of the benefits of alternative dispute resolution. By bringing the two sides to a dispute together to seek a mutual solution, alternative dispute resolution can reduce both conflict and costs and lead to a settlement that leaves both sides satisfied. For this reason, I have incorporated alternative dispute resolution processes into the Office's mechanisms for addressing complaints.

During the past year, I responded to a number of enquiries from concerned individuals. I can report, however, that no formal complaints were received by my Office.

Anonymous Allegations

One option open to me in reviewing the activities of CSE is to guarantee anonymity to people, particularly current or former employees, who come to me with allegations of illegal activity by CSE. Some observers believe such an offer would enhance my ability to determine whether such activities were taking place.

I do not believe guaranteed anonymity for accusers is the right way to go. This approach would have the potential to poison the operating environment at CSE, or at any other institution with such a guarantee. Managers and co-workers could easily become reluctant to offer necessary criticisms and critiques of the work of other employees for fear that an offended employee could make anonymous unfounded accusations against them.

For these reasons, the complaints procedures I have established for this Office do not shield the identity of people who bring forth allegations of illegal activity by CSE. It is my belief that, by putting the appropriate mechanisms in place in an environment designed to address issues constructively, complainants will feel compelled to come forward, in good faith, to raise legitimate concerns. At the same time, I will not hesitate to use all the authority of my Office to ensure that complainants acting in good faith do not suffer reprisals from any quarter, regardless of the ultimate disposition of the issues they raise.

Building Relationships

The ability of my Office to review the activities of CSE can be enhanced by the relationships we have with stakeholders beyond CSE itself. During 1999-2000, two developments served to strengthen this Office's relationships with others.

DND Ombudsman

In June 1999, the Minister of National Defence announced the mandate of André Marin, the Ombudsman for the Department of National Defence (DND) and the Canadian Forces. The Ombudsman is designated to act on the Minister's behalf, independent of the chain of command, as a neutral and objective sounding board, mediator and reporter on matters related to the Department of National Defence and the Canadian Forces.

Because the Communications Security Establishment is an agency of DND, there is potential overlap between my role and that of the Ombudsman. In the autumn of 1999, Mr. Marin and I met to discuss our respective mandates as well as to establish clear boundaries and procedures for cooperation between our two Offices. We agreed the Ombudsman has an important role in addressing issues raised by CSE employees, but that role does not extend to activities related to the mandate of CSE. In other words, it is my responsibility to deal with issues involving CSE's SIGINT or ITS activities.

We are confident that, between the two of us, we can effectively and efficiently address any concerns that may arise about CSE.

International Conference

At the international level, the second conference of Inspectors-General and Review Agencies, which took place in Ottawa in June 1999, gave me an opportunity to discuss mutual interests with colleagues from Australia, New Zealand, the United Kingdom, the United States, Belgium and South Africa. The event was hosted by Canada's Security Intelligence Review Committee, the agency responsible for reviewing the Canadian Security Intelligence Service. The first such conference took place in Canberra, Australia in 1997.

Among the topics of discussion at the conference were relations between review organizations and legislators, and relationships with the media. The participation of Canadian parliamentarians and journalists made these sessions particularly informative. Equally valuable were the formal and informal exchanges with people from other countries who have responsibilities similar to my own. By comparing experiences, we learned how others have addressed the challenges we share.

The Future of Review for CSE

In prepared remarks to the conference of Inspectors-General and Review Agencies, I noted that over the past decade or two, many of our governments have increased their efforts to monitor and report on the lawfulness of their intelligence agencies – a trend I said was likely to continue. Government actions in this regard have been deliberate and carefully thought out, in keeping with the importance and sensitivity of intelligence activities, but the direction is clearly toward greater openness and increased accountability.

I noted that a key issue in the Canadian context is whether the Government of Canada should introduce legislation for CSE. I observed that any such legislation would likely include the creation of a permanent review mechanism in place of my fixed-term appointment by Order in Council.

As I have said before, I believe that legislation for CSE would be an appropriate development. However, if and when the government decides to move in this direction, it should act with the same caution and deliberation that have been the hallmarks of western governments in dealing with their intelligence agencies. In my view, the arrangements now in place to review CSE are entirely effective, and there is no urgency to alter them independent of the larger issue of whether CSE should have a legislative base. Permanent review arrangements should reflect the foreign intelligence nature of the work of CSE and the degree to which CSE could infringe on the rights and privacy of Canadians in fulfilling its mandate.

My New Website

Last year saw the launch of the official website of the Office of the Communications Security Establishment Commissioner. My objective with the site is to make information about this Office more readily available to the growing number of Canadians with access to the Internet. The site provides background on the mandate and functions of the Commissioner and access to my annual reports. The website address is http://csec-ccst.gc.ca.

People and Places

One of the challenges facing CSE in the past was that its employees were scattered in several buildings in Ottawa. That situation improved with the recent acquisition of the former Canadian Broadcasting Corporation headquarters, which is close to the main CSE facility, the Sir Leonard Tilley Building. The new building – now named the Edward Drake Building in honour of the first head of CSE's predecessor organization, the Communications Branch of the National Research Council – will allow CSE to consolidate most of its operations in the two buildings, under the leadership of its new Chief, Mr. D. Ian Glen.

On a separate note, the government and the people of Canada lost an outstanding public servant with the death in August 1999 of Mr. John Tait. I had the honour of knowing Mr. Tait when he was Deputy Minister of Justice and I was Chief Justice of Quebec. When I took on this job, he was the Coordinator of Security and Intelligence in the Privy Council Office and thereby the Deputy Minister responsible for CSE's policy and operations. Among his many other contributions to the government was a 1997 report on public service values and ethics, produced by a task force that he chaired. The document, now widely known as the Tait Report, has helped generate a strengthening of values-based governance in the Government of Canada.

CANADA

PRIVY COUNCIL • CONSEIL PRIVÉ

P.C. 1999-1048
June 8, 1999

His Excellency the Governor General in Council, on the recommendation of the Minister of National Defence, pursuant to Part II of the *Inquiries Act*, hereby authorizes the Minister of National Defence (in this order referred to as "the Minister")

(*a*) to re-appoint the Honourable Claude Bisson of Montreal, Quebec, for a period of three years, as a commissioner ("the Commissioner") to review the activities of the Communications Security Establishment ("CSE") for the purpose of determining whether those activities are in compliance with the law;

(*b*) to authorize the Commissioner to commence that review on his own initiative or at the request of the Minister;

(*c*) to authorize the Commissioner to investigate any complaint, concerning the lawfulness of CSE activities, made by any individual who is a Canadian citizen or a permanent resident of Canada;

(*d*) to authorize the Commissioner not to investigate complaints for which, in the Commissioner's opinion, other avenues of redress are established by statute;

(*e*) to specifically authorize the Commissioner to inform any complainant of the results of his investigation, ensuring that no classified information is disclosed to the complainant;

(*f*) to direct the Commissioner to inform the Minister and the Attorney General of Canada of any CSE activity that the Commissioner believes may not be in compliance with the law;

.../2

(*g*) to direct the Commissioner to submit to the Minister, once each year and in both official languages, a report on the Commissioner's activities and findings that are not classified, which report the Minister will table in Parliament;

(*h*) to authorize the Commissioner, at any time the Commissioner considers it advisable, to submit a report containing classified information to the Minister;

(*i*) to direct the Commissioner, before submitting any report to the Minister, to consult with the Deputy Secretary to the Cabinet (Security and Intelligence) at the Privy Council Office for the purpose of ensuring compliance with all security requirements and the preservation of the secrecy of sources of security and intelligence information and of the security of information provided to Canada in confidence by other nations;

(*j*) to direct the Commissioner and all persons engaged on his behalf take an oath of secrecy and comply with all applicable government security requirements;

(*k*) to authorize the Commissioner to engage the services of any staff, advisors and counsel that he considers necessary to assist him in the performance of his duties and functions at such rates of remuneration and reimbursement as may be approved by the Treasury Board;

.../3

(*l*) to fix the remuneration of the Commissioner at the per diem rate set out in the annexed schedule, which rate is within the range of $400 to $500; and

(*m*) to authorize that the Commissioner be paid reasonable travel and living expenses incurred by him in the performance of his duties and functions while absent from his ordinary place of residence, in accordance with Treasury Board travel directives;

effective June 19, 1999.

CERTIFIED TO BE A TRUE COPY-COPIE CERTIFIÉE CONFORME

CLERK OF THE PRIVY COUNCIL-LE GREFFIER DU CONSEIL PRIVÉ

Commissaire du Centre de la sécurité des télécommunications

Canada

Bureau du Commissaire du Centre de la sécurité des télécommunications
C.P. 1984, Succursale « B »
Ottawa (Ontario)
K1P 5R5

Tél. : (613) 992-3044
Téléc. : (613) 992-4096

© Ministre des Travaux publics et des Services gouvernementaux Canada 2000
ISSN 1206-7490
N° de cat. D95-2000

Communications Security
Establishment Commissioner

The Honourable Claude Bisson, O.C.

CANADA

Commissaire du Centre de la
sécurité des télécommunications

L'honorable Claude Bisson, O.C.

Mai 2000

L'honorable Arthur C. Eggleton, C.P.
Ministre de la Défense nationale
Édifice Mgén G.R. Pearkes, 13e étage
101, promenade Colonel By, tour nord
Ottawa (Ontario)
K1A 0K2

Monsieur le Ministre,

Conformément à l'alinéa g) du décret C.P. 1999-1048 prévoyant le renouvellement de ma nomination au poste de commissaire du Centre de la sécurité des télécommunications, j'ai le plaisir de vous soumettre mon rapport annuel pour l'année 1999-2000, qui fait état de mes activités et constatations, pour présentation au Parlement.

Je vous prie d'agréer, Monsieur le Ministre, l'assurance de ma haute considération.

Claude Bisson

P.O. Box/C.P. 1984, Station "B"/Succursale «B»
Ottawa, Canada
K1P 5R5
(613) 992-3044 Fax: (613) 992-4096

TABLE DES MATIÈRES

Nouveau mandat 1

Travaux d'examen en 1999-2000 2

- Enquêtes et plaintes internes 2
- Renseignements électromagnétiques sur l'étranger 2

  Le cycle du renseignement 3

  Collecte de renseignements « par une seconde partie » 5
- Sécurité des technologies de l'information 6

Budget et personnel 8

Constatations faites en 1999-2000 8

La fonction relative aux plaintes 9

- Allégations anonymes 10

Développement de relations 11

- Ombudsman du MDN 11
- Conférence internationale 12

L'avenir de l'examen pour le CST 13

Mon nouveau site Web 14

Personnel et locaux 14

Annexe : Décret C.P. 1999-1048 15

Nouveau mandat

J'ai, depuis quatre ans, la responsabilité d'examiner les activités du Centre de la sécurité des télécommunications (CST) et de faire rapport au ministre de la Défense nationale sur leur légalité.

Mon premier mandat de trois ans était énoncé dans un décret pris par le gouvernement du Canada en 1996 en vertu de la *Loi sur les enquêtes*. Le 15 juin 1999, le ministre de la Défense nationale a annoncé que le gouvernement avait renouvelé mon mandat pour trois autres années et l'avait étendu en élargissant mon pouvoir de répondre aux plaintes au sujet du CST. Une copie du nouveau décret figure à l'annexe A du présent rapport.

Ce rapport annuel, qui est mon quatrième, couvre la première année de mon deuxième mandat, jusqu'à la fin de l'année financière du gouvernement, soit le 31 mars 2000.

Le travail d'examen des activités du CST est important et nécessaire dans une société démocratique. Le CST, qui est un organisme du ministère de la Défense nationale, fournit au gouvernement du Canada des renseignements électromagnétiques sur des pays étrangers (SIGINT) qu'il obtient en recueillant et en analysant leurs transmissions par radio, par radar et par d'autres moyens électroniques. Dans le cadre de son programme de sécurité des technologies de l'information, il donne en outre des conseils sur la sécurité des technologies de l'information du gouvernement.

Le CST existe depuis plus de 50 ans. Au cours de cette période, il a mis au point des moyens techniques très perfectionnés en vue d'exécuter son mandat. L'une de mes fonctions consiste à examiner ses activités afin de m'assurer qu'il n'emploie pas ces moyens de manières contraires aux lois du Canada.

Travaux d'examen en 1999-2000

Au cours de l'année écoulée, j'ai présenté quatre rapports classifiés au ministre de la Défense nationale. L'un de ceux-ci réexaminait la question des enquêtes et des plaintes internes. Les trois autres présentaient les résultats d'examens d'activités menées par le CST en matière de renseignement sur l'étranger et de sécurité des technologies de l'information. Toutes ces études comportaient un examen des paramètres juridiques régissant les activités du CST, des politiques et pratiques connexes et des systèmes et mécanismes de responsabilisation en place au sein de l'organisme. Aucune n'a révélé de problème ayant trait à des activités illégales.

Enquêtes et plaintes internes

Lors de mon premier examen des enquêtes et des plaintes internes, en 1997-1998, j'ai constaté que la plupart avaient rapport à des questions comme les infractions à la sécurité et que, dans aucun cas, le CST ne s'était livré à des activités illégales dans l'exécution de son mandat. J'ai fait la même constatation cette année. Dans l'intervalle, le CST a mis en œuvre un bon nombre de nouvelles politiques et initiatives internes destinées à sensibiliser davantage le personnel à la sécurité. Ces mesures semblent avoir été efficaces, en ce sens que le nombre des incidents ayant nécessité des enquêtes internes a été beaucoup moins élevé au cours de l'année dernière qu'en 1997-1998.

Renseignements électromagnétiques sur l'étranger

Dans mon examen des activités du CST en matière de renseignement électromagnétique sur l'étranger au cours de l'année écoulée, j'ai remarqué que l'on améliorait et révisait constamment les politiques et directives en la matière, compte tenu de l'évolution dans le domaine des communications. J'ai en outre relevé les nouvelles initiatives instaurées par le CST afin d'accroître sa capacité de gérer ses activités liées au SIGINT et de rendre compte de celles-ci.

J'ai fait particulièrement attention, cette année, à examiner non seulement *la nature* des renseignements que le CST recueille et conserve, mais aussi *la façon* dont ses fonds de renseignements sont créés. Cela m'a permis de mieux connaître et comprendre certains des moyens très spécialisés et très techniques employés pour réduire au minimum la probabilité que des communications privées de Canadiens se retrouvent dans les fonds de renseignements du CST. Je suis en mesure d'affirmer qu'à ce jour, je suis convaincu que, dans le contexte technique actuel, le CST emploie des mesures appropriées pour protéger la vie privée des Canadiens.

Le cycle du renseignement

Dans mon rapport de l'année dernière, je mentionnais que le moteur des activités du CST est son mandat de répondre aux besoins de renseignement sur l'étranger établis par le gouvernement du Canada, et non pas les capacités de la technologie dont il dispose.

Ces besoins, qui prennent la forme des priorités de la communauté canadienne du renseignement en matière de renseignement sur l'étranger, sont établis annuellement par un groupe de ministres du Cabinet, dont les responsabilités touchent à la sécurité intérieure et extérieure du Canada. La définition des priorités du gouvernement du Canada est la première étape de ce que la communauté du renseignement est convenue d'appeler le « cycle du renseignement ». Il vaut la peine d'examiner brièvement ce cycle et le rôle qu'y joue le CST.

Les priorités du gouvernement du Canada en matière de renseignement sur l'étranger forment la base du programme annuel de SIGINT du CST. Ces priorités sont communiquées officiellement au CST par le sous-secrétaire du Cabinet (sécurité et renseignement), du Bureau du Conseil privé. Le CST les utilise ensuite pour déterminer quels

renseignements il cherche à tirer de ses propres activités ou de celles de ses partenaires aux États-Unis, au Royaume-Uni, en Australie et en Nouvelle-Zélande.

Parallèlement, le CST doit s'assurer que l'on prend toujours les mesures voulues pour réduire au minimum la probabilité d'intercepter les communications privées de Canadiens.

Ensuite, le CST reçoit le flux de transmissions de nombreuses sources, tant les siennes propres que celles de ses partenaires. Ces transmissions sont ensuite traitées, analysées et évaluées par rapport aux priorités du gouvernement en matière de renseignement. Les renseignements qui en résultent sont diffusés aux ministères chargés de protéger les intérêts du Canada sur les plans de la sécurité, du renseignement, de l'économie et de la défense.

La diffusion des renseignements est facilitée par le personnel du CST, qui est bien informé et qui offre à quelque 800 décideurs de haut niveau de l'administration publique un service de prestation de renseignement adapté et opportun sur des questions nouvelles ou courantes. Ces contacts réguliers avec les utilisateurs de ses produits de renseignement permettent au Centre de mettre à jour les besoins et de prendre en compte les réactions des clients dans son processus de production.

Le cycle du renseignement me fournit un cadre pour examiner les activités du CST. Je peux vérifier la légalité de ces activités à chaque étape du cycle. Grâce à ce travail, je me tiens au courant des moyens et pratiques en matière de collecte de renseignements sur l'étranger, du traitement des signaux, de l'analyse des signaux et des renseignements, et de la diffusion des produits du renseignement aux clients du CST à l'administration fédérale.

J'estime que la profusion d'information transportée par les réseaux de communications mondiaux accroît la nécessité de veiller à protéger la vie privée des Canadiens. Je continue à travailler pour reconnaître et comprendre les nombreuses initiatives technologiques qui appuient la collecte de renseignements. J'approfondis en outre ma connaissance de la façon dont on applique certaines de ces initiatives. Toutefois, ce qui m'intéresse dans le cycle du renseignement, c'est la reconnaissance et l'examen de toutes les applications et initiatives techniques que le CST utilise pour éviter, ou à tout le moins réduire au minimum, la probabilité que des communications privées de Canadiens se retrouvent dans ses fonds de renseignements.

Je suis à même de déclarer que le CST a pris des initiatives pour perfectionner ses moyens techniques afin d'assurer la protection des communications privées des Canadiens. Le CST est au courant de l'intérêt que je porte à cette question et de l'importance que j'attache à l'évaluation de sa conformité à cet égard. J'encourage les initiatives de recherche et de développement du CST dans notre contexte technologique en évolution rapide.

Collecte de renseignements « par une seconde partie »

Comme je l'ai mentionné plus haut, le CST reçoit des renseignements électromagnétiques recueillis par d'autres gouvernements. Il fournit également à ceux-ci des renseignements qu'il a lui-même recueillis. Ces accords de partenariat avec les États-Unis, le Royaume-Uni, l'Australie et la Nouvelle-Zélande ont été établis au cours de la Deuxième Guerre mondiale et maintenus pendant toute la durée de la guerre froide. Lorsqu'un pays fournit ainsi des signaux à un autre pays, on parle de collecte de renseignements « par une seconde partie ».

Les gouvernements des pays qui participent à cet échange de renseignements ont des politiques destinées à protéger la vie privée de leurs citoyens.

En particulier, chaque gouvernement a convenu de ne pas effectuer, pour le compte d'une seconde partie, de travail de collecte qui serait illégal dans le pays de cette seconde partie. Autrement dit, ils ne font pas indirectement ce qu'ils ne peuvent pas faire directement.

Je me suis fait un devoir de me familiariser avec ces rapports de collaboration en étudiant non seulement les politiques communes, mais encore les pratiques. J'ai procédé à un échantillonnage de la documentation et j'ai eu accès à certains des systèmes qui appuient la collecte et l'échange de renseignements. J'ai actuellement la conviction que le CST prend toutes les mesures raisonnables pour sauvegarder le caractère privé des communications des Canadiens.

Sécurité des technologies de l'information

Au cours des quatre dernières années, j'ai concentré une bonne partie de mon travail sur les activités de SIGINT du CST. Toutefois, celui-ci joue un autre rôle important au sein de l'administration fédérale. Dans le cadre de son mandat touchant la sécurité des technologies de l'information (STI), le CST donne en effet des conseils au gouvernement sur la façon de préserver la sécurité lorsqu'il a recours à ces technologies.

Cette année, mon bureau a procédé à un examen en profondeur du programme de STI afin de déterminer si ses activités étaient légales. On a d'abord examiné les pouvoirs et le mandat du CST en matière de STI, tels qu'ils sont prévus dans les directives données au chef du CST. On a ensuite examiné le cadre de contrôle de la gestion établi pour régir la conduite et l'exécution des activités de STI. On a analysé en troisième lieu les facteurs liés au contexte et les circonstances nouvelles qui influent sur les besoins du gouvernement en matière de sécurité. On a enfin examiné les stratégies, les plans, les opérations et les projets en regard du modèle établi grâce aux étapes précédentes afin de cerner les questions ou activités à étudier plus avant.

On n'a découvert aucune preuve d'activité illégale. Toutefois, cet examen a mis au jour plusieurs faits pertinents :

- La tendance de l'Administration et du secteur privé à recourir de plus en plus au commerce électronique et à fournir leurs services par voie électronique transforme radicalement le programme de STI. En effet, celui-ci était auparavant axé sur la protection des renseignements classifiés d'un petit nombre de clients de l'État, mais ses responsables sont de plus en plus appelés à donner des conseils sur la protection de renseignements non classifiés mais de nature délicate, dont les opérations de commerce électronique qui sous-tendent nombre de programmes et d'activités de l'État.
- Si le gouvernement veut que les Canadiens aient confiance dans le commerce électronique et l'infrastructure qui le rend possible, il doit pouvoir offrir des solutions « canadiennes » aux préoccupations relatives à la sécurité. Le CST possède les moyens voulus pour jouer un rôle clé à cet égard, mais il doit recevoir des instructions claires du gouvernement sur cette question délicate.
- Par exemple, un moyen efficace de vérifier la sécurité de l'infrastructure d'information consiste à essayer d'en pénétrer les barrières (autrement dit à en éprouver les « pare-feu »). On parle alors de « piraterie éthique ». Le CST ne pénètre pas de systèmes actifs de cette manière, car cela pourrait mettre au jour des données personnelles, ce qui aurait des répercussions sur la vie privée. Toutefois, cela a pour résultat que les systèmes de technologies de l'information essentiels ne sont pas vérifiés par rapport à la gamme complète des menaces auxquelles ils sont exposés.

Je surveillerai désormais de près la participation du programme de STI à ces activités pour m'assurer qu'elles respectent les limites actuelles.

J'encouragerais par ailleurs le gouvernement à donner des instructions claires au CST quant au rôle qu'il devrait jouer pour assurer la sécurité de l'infrastructure d'information du Canada.

Budget et personnel

Le budget qui m'avait été alloué pour l'année 1999-2000 a été porté à 635 500 $ afin de couvrir des dépenses supplémentaires, dont des services de conseils juridiques, liées à l'expansion de mon mandat touchant les plaintes. Je suis à même de déclarer que les dépenses effectivement engagées ont respecté les limites de ce budget.

Conformément à la pratique établie au cours de mon premier mandat, j'ai continué à m'appuyer sur deux employées à plein temps et à retenir par contrat les services de spécialistes de questions particulières. À l'heure actuelle, six contractuels effectuent des travaux spécialisés selon cette formule, et tous possèdent l'autorisation de sécurité nécessaire à leur travail.

Comme je l'ai mentionné par le passé, j'estime disposer des ressources financières et en personnel voulues pour m'acquitter du mandat qui m'a été confié.

Constatations faites en 1999-2000

À la lumière des résultats de notre examen et de notre analyse, je suis d'avis que le CST s'est conformé à la loi dans l'exercice des activités prévues par son mandat au cours de la période examinée. Je suis par ailleurs convaincu qu'il n'a pas ciblé les communications de citoyens canadiens ni de résidents permanents du Canada.

Ces constatations rejoignent celles que j'ai faites ces dernières années, depuis la création de mon bureau. Grâce à mon travail d'étude et d'examen, je connais et comprends de mieux en mieux la façon dont le CST exerce les activités prévues par son mandat. À mesure que j'approfondis cette

connaissance, je suis de plus en plus sûr de ma méthode d'évaluation quant à la légalité de ces activités. L'assurance croissante avec laquelle je peux formuler mes constatations est particulièrement importante à mes yeux.

La nature même des activités de renseignement sur l'étranger soulève des questions, et parfois des préoccupations, chez les citoyens. Et je peux témoigner de la complexité du cycle du renseignement sur les plans technique, juridique et éthique. Je pense par conséquent que l'existence de mon bureau depuis 1996 a constitué un ajout nécessaire et opportun à la communauté canadienne du renseignement. J'ai constaté que, depuis 1996, les politiques et méthodes du CST et, par-dessus tout, ses pratiques reflètent la présence de mon bureau et mes paramètres d'examen tels qu'ils ont été établis par le gouvernement du Canada.

Les capacités croissantes de mon bureau, alliées à l'amélioration des politiques et des pratiques du CST, sont de bon augure pour l'avenir. Néanmoins, j'entends rester vigilant dans l'examen des activités du CST, et je veillerai à ce que nous employions énergiquement ces capacités aussi longtemps que j'occuperai la charge de commissaire.

La fonction relative aux plaintes

L'année écoulée a été la première au cours de laquelle j'ai eu le pouvoir de répondre directement aux personnes qui formulent des plaintes au sujet des activités du CST. Auparavant, mon mandat initial me permettait de recevoir ces plaintes, mais non de faire rapport de mes constatations aux plaignants. J'ai été heureux de voir cette limite supprimée lors du renouvellement de mon mandat.

Afin d'aider le grand public à comprendre le rôle de mon bureau et, en particulier, la fonction relative aux plaintes, nous avons publié une brochure intitulée *Protéger la vie privée des Canadiens*. On y signale que, comme les plaintes peuvent comporter des renseignements de nature délicate

ou toucher la vie privée de Canadiens, mon bureau acceptera uniquement les plaintes qui me seront adressées personnellement par la poste. On peut obtenir des exemplaires de cette brochure sur demande.

Mes antécédents et ma formation dans le domaine de l'arbitrage et de la médiation avant ma nomination au poste de commissaire ont fait de moi un ardent avocat des avantages du règlement extrajudiciaire des différends. En amenant les deux parties à un différend à rechercher ensemble une solution mutuelle, cette formule peut réduire à la fois l'intensité des conflits et les coûts, et mener à un règlement satisfaisant pour l'une comme pour l'autre. C'est pourquoi j'ai intégré les procédés de règlement extrajudiciaire des différends aux mécanismes prévus par mon bureau pour résoudre les plaintes.

Au cours de l'année écoulée, j'ai répondu à un certain nombre de demandes de renseignements de citoyens inquiets. Je suis cependant à même de signaler que mon bureau n'a reçu aucune plainte officielle.

Allégations anonymes

Dans l'examen des activités du CST, j'ai la possibilité de garantir l'anonymat aux personnes qui accusent l'organisme de se livrer à des activités illégales, en particulier s'il s'agit d'employés actuels ou d'ex-employés. De l'avis de certains observateurs, cela accroîtrait ma capacité de déterminer l'existence de telles activités.

Je ne pense pas que ce soit là une bonne façon de procéder. Le fait de garantir l'anonymat aux accusateurs pourrait empoisonner l'atmosphère de travail du CST, ou de toute autre institution qui offrirait une telle garantie. En effet, les gestionnaires et les collègues pourraient facilement en venir à hésiter à formuler des critiques ou des commentaires nécessaires au sujet du travail d'autres employés de crainte que ceux-ci s'offusquent et décident de porter contre eux des accusations anonymes sans fondement.

Pour ces raisons, la procédure de traitement des plaintes que j'ai établie pour mon bureau ne protège pas l'identité des personnes qui présentent des allégations d'activité illégale de la part du CST. J'estime que si l'on met en place les mécanismes appropriés dans un contexte conçu pour aborder les problèmes de manière constructive, les personnes qui ont des sujets de plainte légitimes se sentiront tenues de les présenter en toute bonne foi. Par ailleurs, je n'hésiterai pas à me servir de toute l'autorité attachée à mes fonctions pour m'assurer que les plaignants agissant de bonne foi ne subiront aucune mesure de représailles de quelque provenance que ce soit, indépendamment de la résolution finale des questions qu'ils auront soulevées.

Développement de relations

Les relations qu'entretient mon bureau avec des parties intéressées au delà du CST lui-même peuvent accroître sa capacité d'examiner les activités de cet organisme. Au cours de l'année 1999-2000, deux facteurs ont permis de renforcer les relations de mon bureau avec d'autres parties.

Ombudsman du MDN

En juin 1999, le ministre de la Défense nationale a rendu public le mandat de M. André Marin, ombudsman du ministère de la Défense nationale (MDN) et des Forces canadiennes. Celui-ci est désigné pour agir au nom du Ministre, indépendamment de la chaîne de commandement; il doit, de manière neutre et objective, formuler des avis, jouer un rôle de médiateur et faire rapport sur des questions se rapportant au ministère de la Défense nationale et aux Forces canadiennes.

Comme le Centre de la sécurité des télécommunications relève du MDN, il existe une possibilité de chevauchement entre mon rôle et celui de l'ombudsman. À l'automne de 1999, M. Marin et moi-même nous sommes réunis pour examiner nos mandats respectifs et pour établir des limites claires et des méthodes de coopération entre nos deux bureaux. Nous avons convenu que l'ombudsman a

un rôle important à jouer pour résoudre les questions soulevées par des employés du CST, mais que ce rôle ne s'étend pas aux activités liées au mandat de l'organisme. Autrement dit, c'est à moi qu'il appartient de traiter les questions se rapportant aux activités du CST en matière de SIGINT et de STI.

Nous sommes persuadés de pouvoir, de part et d'autre, résoudre réellement et efficacement toute préoccupation pouvant être soulevée au sujet du CST.

Conférence internationale

Au palier international, la deuxième conférence des inspecteurs généraux et des organismes de surveillance, qui s'est tenue à Ottawa en juin 1999, m'a fourni l'occasion de discuter de questions d'intérêt mutuel avec des collègues de l'Australie, de la Nouvelle-Zélande, du Royaume-Uni, des États-Unis, de la Belgique et de l'Afrique du Sud. Le Comité de surveillance des activités du renseignement de sécurité du Canada, qui est chargé de surveiller le Service canadien du renseignement de sécurité, en était l'hôte. La première de ces conférences avait eu lieu à Canberra (Australie) en 1997.

Citons parmi les sujets discutés à la conférence les relations entre les organismes de surveillance et les législateurs, et les relations avec les médias. La participation de parlementaires et de journalistes canadiens a fait que ces séances ont été particulièrement informatives. Les échanges de vues officiels et informels avec des gens d'autres pays qui ont des responsabilités semblables aux miennes ont également été précieux. En comparant nos expériences respectives, nous avons vu comment d'autres personnes ont relevé les mêmes défis que ceux auxquels nous sommes confrontés.

L'avenir de l'examen pour le CST

Dans une allocution rédigée en vue de la conférence des inspecteurs généraux et des organismes de surveillance, je mentionnais que, au cours des quelque 10 à 20 dernières années, nombre de nos gouvernements avaient intensifié leurs efforts de surveillance et de rapports touchant la légalité des activités de leurs services de renseignement, et je disais que cette tendance allait probablement se maintenir. Les mesures prises par les gouvernements à cet égard ont été mûrement réfléchies et conçues avec grand soin, compte tenu de l'importance et du caractère délicat des activités de renseignement, mais elles tendent manifestement vers une plus grande ouverture et une responsabilisation accrue.

J'ai signalé qu'une des questions clés qui se posent dans le contexte canadien consiste à savoir si le gouvernement du Canada devrait adopter une loi pour régir l'activité du CST. J'ai fait remarquer que, le cas échéant, cette loi prévoirait probablement la création d'un mécanisme d'examen permanent qui remplacerait ma nomination par décret pour une durée déterminée.

Comme je l'ai déjà dit, je pense qu'il serait opportun d'établir une loi visant le CST. Toutefois, si jamais le gouvernement décide d'agir dans ce sens, il devrait procéder avec la même prudence et la même réflexion que celle avec laquelle les gouvernements occidentaux ont abordé la surveillance de leurs services de renseignement. À mon avis, le mécanisme actuellement en place pour examiner les activités du CST est tout à fait efficace, et il n'y a aucune urgence à le modifier hors du contexte plus large de l'adoption éventuelle d'une loi visant cet organisme. Tout mécanisme d'examen permanent devrait tenir compte du fait que les travaux du CST ont trait aux renseignements sur l'étranger et de la mesure dans laquelle l'organisme pourrait porter atteinte aux droits et à la vie privée des Canadiens dans l'exécution de son mandat.

Mon nouveau site Web

Le site Web officiel du Bureau du commissaire du Centre de la sécurité des télécommunications est entré en service au cours de l'année dernière. Mon objectif, en établissant ce site, est de permettre au nombre croissant de Canadiens qui ont accès à Internet d'obtenir plus facilement de l'information au sujet de mon bureau. On y trouve des renseignements de base sur le mandat et les fonctions du commissaire, ainsi que mes rapports annuels. L'adresse en est la suivante : http://csec-ccst.gc.ca.

Personnel et locaux

L'un des problèmes auxquels le CST a fait face par le passé a été l'éparpillement de ses employés dans plusieurs édifices à Ottawa. L'achat récent de l'ancien siège de la Société Radio-Canada, qui se trouve à proximité de l'édifice Sir Leonard Tilley, principale installation du CST, a amélioré cette situation. Le nouvel immeuble — maintenant baptisé édifice Edward Drake en l'honneur du premier dirigeant de l'ancêtre du CST, la Direction des communications du Conseil national de recherches — permettra à l'organisme de regrouper la plupart de ses activités dans les deux édifices, sous la direction de son nouveau chef, M. D. Ian Glen.

Dans un autre ordre d'idées, le gouvernement et la population du Canada ont perdu un fonctionnaire éminent lors du décès de M. John Tait, en août 1999. J'ai eu l'honneur de faire la connaissance de M. Tait lorsqu'il était sous-ministre de la Justice et que j'occupais la charge de juge en chef du Québec. Lorsque j'ai pris mes fonctions actuelles, il était coordonnateur de la sécurité et du renseignement au Bureau du Conseil privé et, de ce fait, sous-ministre responsable de la politique et des activités du CST. L'une de ses nombreuses contributions à l'administration fédérale a été un rapport sur les valeurs et l'éthique de la fonction publique, produit et publié en 1997 par un groupe de travail qu'il avait présidé. Ce document, maintenant appelé communément rapport Tait, a contribué à renforcer la gestion des affaires publiques fondée sur des valeurs au sein du gouvernement du Canada.

CANADA

PRIVY COUNCIL • CONSEIL PRIVÉ

C.P. 1999-1048
8 juin 1999

Sur recommandation du ministre de la Défense nationale et en vertu de la partie II de la *Loi sur les enquêtes*, Son Excellence le Gouverneur général en conseil autorise le ministre de la Défense nationale (le « ministre ») :

a) à reconduire l'honorable Claude Bisson, de Montréal (Québec), dans ses fonctions de commissaire du Centre de la sécurité des télécommunications (le « CST ») pour une période de trois ans pendant laquelle il examinera les activités du CST et s'assurera qu'elles sont conformes à la loi;

b) à autoriser le commissaire à entreprendre cet examen de sa propre initiative ou à la requête du ministre;

c) à autoriser le commissaire à instruire toute plainte concernant la légalité des activités du CST que pourrait déposer un citoyen canadien ou un résident permanent du Canada;

d) à autoriser le commissaire à ne pas instruire une plainte lorsque, de l'avis de celui-ci, il existe d'autres recours légaux;

e) à autoriser expressément le commissaire à informer toute personne ayant déposé une plainte des résultats de l'enquête qui a été effectuée, en prenant soin de ne divulguer aucun renseignement confidentiel à cette personne;

f) à enjoindre au commissaire de signaler au ministre et au procureur général du Canada toute activité du CST qu'il estime ne pas être conforme à la loi;

.../2

g) à enjoindre au commissaire de présenter au ministre, une fois l'an et dans les deux langues officielles, un rapport sur ses activités et ses constatations qui ne sont pas de nature confidentielle, le rapport devant être déposé par le ministre au Parlement;

h) à autoriser le commissaire à présenter au ministre, et ce à tout moment jugé opportun par le commissaire, un rapport contenant des renseignements confidentiels;

i) à enjoindre au commissaire, avant la présentation de tout rapport au ministre, de consulter le sous-secrétaire du Cabinet (Sécurité et renseignement) au Bureau du Conseil privé pour s'assurer que toutes les exigences relatives à la sécurité sont respectées, y compris la confidentialité des sources et la protection des renseignements obtenus de pays étrangers;

j) à exiger que le commissaire et toutes les personnes engagées pour son compte prononcent un serment de discrétion et se conforment à toutes les exigences du gouvernement en matière de sécurité;

k) à autoriser le commissaire à retenir les services de toute personne dont il juge avoir besoin pour l'assister dans ses fonctions, aux taux de rémunération et d'indemnisation que peut approuver le Conseil du Trésor;

.../3

l) à fixer la rémunération du commissaire au taux journalier établi dans l'annexe ci-jointe, lequel se situe entre 400 $ et 500 $;

m) à autoriser le remboursement des frais de transport et de séjour raisonnables engagés par le commissaire lorsque l'exercice de ses fonctions l'amène à s'éloigner de son lieu de résidence habituel, conformément aux directives du Conseil du Trésor concernant les déplacements;

à compter du 19 juin 1999.

CERTIFIED TO BE A TRUE COPY–COPIE CERTIFIÉE CONFORME

CLERK OF THE PRIVY COUNCIL–LE GREFFIER DU CONSEIL PRIVÉ